

UNITED STATES DISTRICT COURT

for the

Western District of Wisconsin

In the Matter of the Search of)

(Briefly describe the property to be searched
or identify the person by name and address))

2024 Tennyson Lane #420, Madison, Wisconsin 53704)

Case No. 23-mj-54)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Western District of Wisconsin

(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 5/2/2023 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of

Date and time issued: 4/18/2023 1:26 PM



Judge's signature

City and state: Austin, Texas

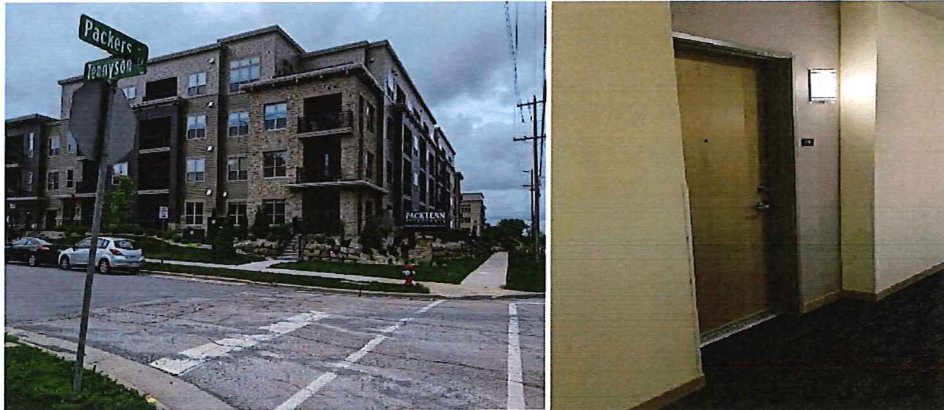
Magistrate Judge Andrew Wiseman

Printed name and title

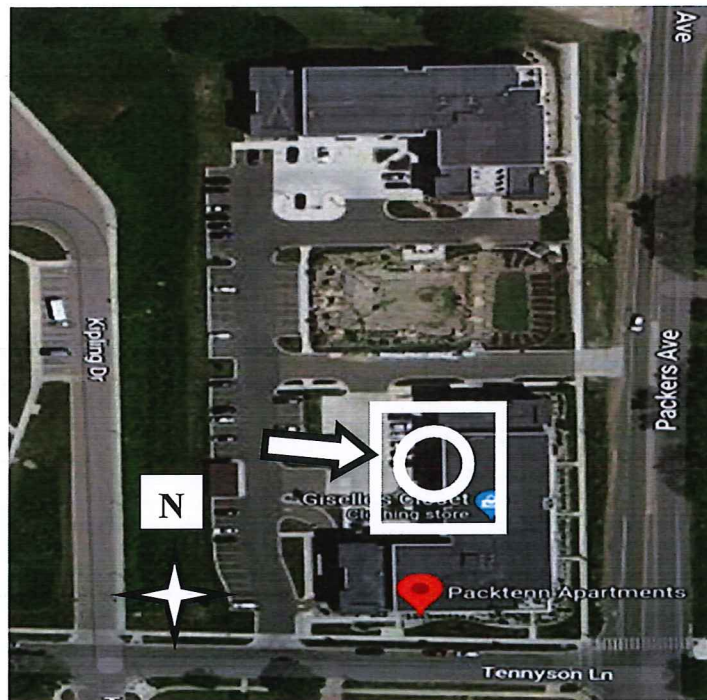
ATTACHMENT A

PROPERTY TO BE SEARCHED

The Subject Premises, **2024 Tennyson Lane #420, Madison, WI 53704**, is an apartment within the PackTenn apartment complex located at the northwest corner of the intersection of Tennyson Lane and Packers Avenue. The main entrance to the apartment complex is on the north side of Tennyson Lane. The Subject Premises is located within the building on the fourth floor. The following are recent photographs of the apartment complex entrance and the front door of the Subject Premises:



The following is an aerial image recently extracted from Google Maps of the general location of the PackTenn apartment complex in which the Subject Premises is situated. The PackTenn apartment complex is identified by a white rectangle and a white arrow. The white rectangle and white arrow are used merely to indicate the general location of the apartment complex within which the Subject Premises is situated and are not intended to define the actual or exact legal boundaries of the Subject Premises or the boundaries of the authorized search location.



ATTACHMENT B

ITEMS TO BE SEIZED AND SEARCHED

Items to be seized include all evidence relating to violations of 18 U.S.C. § 912 (Impersonating a Federal Officer) and 18 U.S.C § 2261A (Stalking). This evidence includes the following:

1. Any badges, identification documents, identity cards, insignia, seals, or records purporting to be issued by any department of the United States federal government or any state or local law enforcement entity, and any records or documentation (including electronic records or documentation) bearing the seal or insignia of any department or agency of the United States federal government.
2. Any clothing, equipment (e.g., tactical/utility vest, etc.), that bear indicia (e.g., insignia, lettering, wording, patterns, decals, seals, etc.) associating them with any department or agency of the United States federal government or any state or local law enforcement entity, including generic indicia (e.g., "FBI", "POLICE", "SWAT").
3. Any and all clothing worn by the Subject during the committal of Impersonating a Federal Officer.
4. Any pictures depicting law enforcement affiliations.
5. Evidence of the purchase of law enforcement related items.
6. All evidence relating to research regarding the location or activities of another person in relation to the subject offenses, including internet searches, mapping application searches, and communication with third parties.
7. All evidence of the Subject's travel to Austin, Texas, including but not limited to financial records, travel reservations, rental car receipts, and hotel receipts.

8. All evidence, including emails, text messages, and social media communications, about or to R.S.
9. All evidence regarding the Subject's location history.
10. Any emails regarding or referencing R.S., her location, or efforts to determine her location.
11. Any communications or records, whether physical or electronic, relating to working for/ with, or serving in, any agency or department of the United States federal government, or any state or local law enforcement agency.
12. Electronic devices, including cellular telephones, computers, and other devices containing electronically stored information and/or memory which could potentially contain items of evidence as described in this Attachment B.
13. As used above, the terms "records," "documents," and "items" include all forms of creation or storage, including paper format and electronic/digital format contained on computers* or electronic storage media.**

* For the purpose of this Attachment B and the associated search warrant, "computers" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices capable of performing logical, arithmetic, or storage functions, such as tablet devices, mobile phones, servers, laptop, notebook and desktop computers.

** For the purpose of this Attachment B and the associated search warrant, "electronic storage media" include: hard drives and portable hard drives of any kind, portable data storage devices such as thumb drives, SD cards, and DVD/CDs, network attached storage units, RAM, cyber wallets, cold storage digital currency wallets, or other media that can store digital and electronic data.

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

UNITED STATES DISTRICT COURT

for the

Western District of Wisconsin

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address))

Case No. 23-mj-54

2024 Tennyson Lane #420, Madison, Wisconsin)
 53704)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment A.

located in the Western District of Wisconsin, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. 912 and 2261A

Impersonating a Federal Officer and Stalking

The application is based on these facts:

See attached affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

☐ Sworn to before me and signed in my presence.

☒ Sworn to telephonically and signed electronically.

Date: 4/18/2023 1:26 PM

City and state: Madison, Wisconsin

Applicant's signature

Sandra Jenkins, SA FBI

Printed name and title

Judge's signature

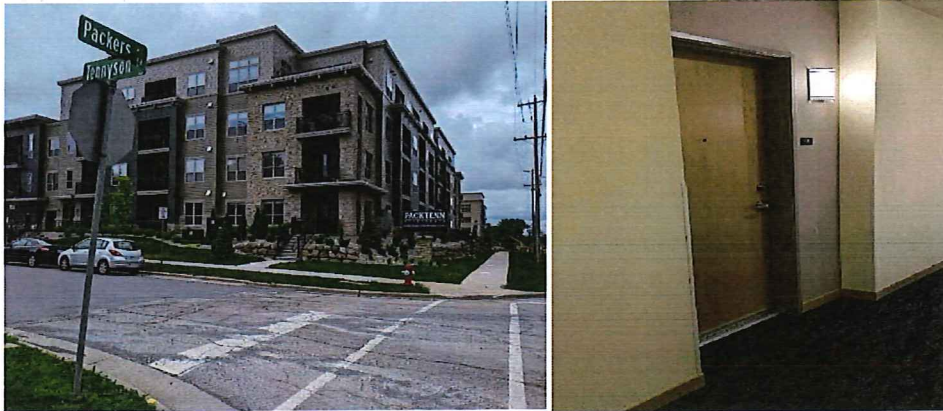
Magistrate Judge Andrew Wiseman

Printed name and title

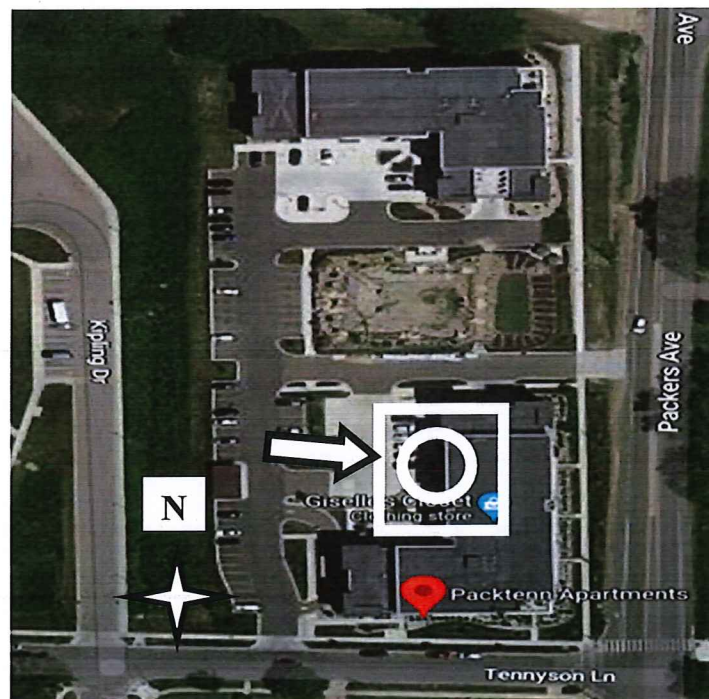
ATTACHMENT A

PROPERTY TO BE SEARCHED

The Subject Premises, **2024 Tennyson Lane #420, Madison, WI 53704**, is an apartment within the PackTenn apartment complex located at the northwest corner of the intersection of Tennyson Lane and Packers Avenue. The main entrance to the apartment complex is on the north side of Tennyson Lane. The Subject Premises is located within the building on the fourth floor. The following are recent photographs of the apartment complex entrance and the front door of the Subject Premises:



The following is an aerial image recently extracted from Google Maps of the general location of the PackTenn apartment complex in which the Subject Premises is situated. The PackTenn apartment complex is identified by a white rectangle and a white arrow. The white rectangle and white arrow are used merely to indicate the general location of the apartment complex within which the Subject Premises is situated and are not intended to define the actual or exact legal boundaries of the Subject Premises or the boundaries of the authorized search location.



ATTACHMENT B

ITEMS TO BE SEIZED AND SEARCHED

Items to be seized include all evidence relating to violations of 18 U.S.C. § 912 (Impersonating a Federal Officer) and 18 U.S.C § 2261A (Stalking). This evidence includes the following:

1. Any badges, identification documents, identity cards, insignia, seals, or records purporting to be issued by any department of the United States federal government or any state or local law enforcement entity, and any records or documentation (including electronic records or documentation) bearing the seal or insignia of any department or agency of the United States federal government.
2. Any clothing, equipment (e.g., tactical/utility vest, etc.), that bear indicia (e.g., insignia, lettering, wording, patterns, decals, seals, etc.) associating them with any department or agency of the United States federal government or any state or local law enforcement entity, including generic indicia (e.g., "FBI", "POLICE", "SWAT").
3. Any and all clothing worn by the Subject during the committal of Impersonating a Federal Officer.
4. Any pictures depicting law enforcement affiliations.
5. Evidence of the purchase of law enforcement related items.
6. All evidence relating to research regarding the location or activities of another person in relation to the subject offenses, including internet searches, mapping application searches, and communication with third parties.
7. All evidence of the Subject's travel to Austin, Texas, including but not limited to financial records, travel reservations, rental car receipts, and hotel receipts.

8. All evidence, including emails, text messages, and social media communications, about or to R.S.
9. All evidence regarding the Subject's location history.
10. Any emails regarding or referencing R.S., her location, or efforts to determine her location.
11. Any communications or records, whether physical or electronic, relating to working for/ with, or serving in, any agency or department of the United States federal government, or any state or local law enforcement agency.
12. Electronic devices, including cellular telephones, computers, and other devices containing electronically stored information and/or memory which could potentially contain items of evidence as described in this Attachment B.
13. As used above, the terms "records," "documents," and "items" include all forms of creation or storage, including paper format and electronic/digital format contained on computers* or electronic storage media.**

* For the purpose of this Attachment B and the associated search warrant, "computers" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices capable of performing logical, arithmetic, or storage functions, such as tablet devices, mobile phones, servers, laptop, notebook and desktop computers.

** For the purpose of this Attachment B and the associated search warrant, "electronic storage media" include: hard drives and portable hard drives of any kind, portable data storage devices such as thumb drives, SD cards, and DVD/CDs, network attached storage units, RAM, cyber wallets, cold storage digital currency wallets, or other media that can store digital and electronic data.

AFFIDAVIT

STATE OF WISCONSIN)

) ss.

DANE COUNTY)

I, Sandra Jenkins, being duly sworn, depose and state as follows:

INTRODUCTION

1. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedures for a search warrant to enter and search the following, which is located in the Western District of Wisconsin:

- a. **The premise located at 2024 Tennyson Lane #420, Madison, Wisconsin 53704**, more specifically described in Attachment A (the "Subject Premises").

As set forth herein, there is probable cause to believe that at, on, or within the Subject Premises there exists evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 912 and 2261A (Impersonating a Federal Officer and Stalking).

2. I am a Special Agent of the Federal Bureau of Investigation (FBI) and have been so employed since June 2022. I am currently assigned to the San Antonio Field Office, Austin Resident Agency, Austin, Texas where I work on the Safe Street Task Force and assist with the Violent Crime squad. My responsibilities include enforcing federal criminal statutes, including investigations involving drugs and illegal narcotics, firearms violations, and violent organized criminal enterprises. As a Federal Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. I am a "federal law enforcement officer" within the meaning of Rule 41(a)(2)(C) of the Federal Rules of

Criminal Procedure. I am engaged in enforcing federal criminal laws and I am authorized by the Attorney General to request a search warrant, among other things.

3. The information contained in this affidavit is based upon information provided by FBI personnel, Austin Police Department (APD) personnel, and other state and local law enforcement officers, public source documents such as police reports, law enforcement databases, physical surveillance, and my own personal investigation. The information contained in this affidavit is submitted for the sole purpose of establishing probable cause for the requested search warrant. As a result, it does not contain every fact known to me concerning the investigation.

FACTS IN SUPPORT OF PROBABLE CAUSE

4. In November 2022, Jack William McQuestion (MCQUESTION) traveled from Madison, Wisconsin to Austin, Texas, with the intent to harass and intimidate the victim, R.S., placing the victim in a reasonable fear of death or serious physical injury. While in Austin, McQUESTION impersonated a federal agent in what I believe was an attempt to abduct R.S.

5. R.S. conducts business via the OnlyFans website and similar online platforms. Generally speaking, OnlyFans is an internet content subscription service used primarily to produce pornography and other adult content. Content creators earn money by uploading videos to the site which can be viewed by paying subscribers. The website reported having 2 million content creators and 130 million users in August 2021. MCQUESTION is suspected to have learned of R.S. through her OnlyFans channel or other similar online platforms.

6. My investigation shows that MCQUESTION made efforts to locate R.S.'s residence prior to November 2022. MCQUESTION's banking records obtained as part of this investigation show he made multiple payments to internet companies that can assist in locating

persons, including 1) multiple White Pages checks; 2) payments made to the open-source search site Hooyu, whose website describes the service as “a unique data visualization tool for investigating people and an identity confirmation service for people to verify the identity of others”; and 3) reoccurring purchases to Spokeo, whose website describes it as a site to “search by name, phone, address, or email to confidentially lookup information about people you know.”

7. MCQUESTION also used the U.S. Postal Service to identify R.S.’s residence. In around November and December 2021, R.S. received two certified letters postmarked November 17, 2021 and December 13, 2021. Both letters had been sent to R.S.’s prior residence in Woodinville, WA and were forwarded to R.S.’s residence in Austin. The return address for both letters was for “Jack McQuestion” and the address was MCQUESTION’s parents’ address in Hartland, WI. Because they were certified letters, the sender would have received notification of the final address to which they were delivered. Bank records for MCQUESTION’s U.S. Bank card show he made a debit purchase at the U.S. Postal Service in the amount of \$7.38 on November 17, 2021 and a second debit purchase at the U.S. Postal Service in the amount of \$6.80 on December 13, 2021. Those dates correspond with the postmark dates on each respective letter and the amounts correspond to the postage cost of each letter.

8. Airline records show that MCQUESTION traveled from Madison, Wisconsin, to Austin, Texas, in August 2022 and back three days after arriving; however, R.S. did not encounter MCQUESTION during that trip.

9. Airline records show that on November 03, 2022, MCQUESTION flew from Madison to Austin by way of Dallas, Texas.

10. While in Austin, MCQUESTION checked in at the Homewood Suites by Hilton located at 13001 Center Lake Drive, Austin, Texas 78753.

11. On November 04, 2022, MCQUESTION travelled to R.S.'s residence and approached her front door. R.S. had a security camera that captured audio and video of MCQUESTION's actions and impersonation of a federal agent. Not all of the audio was captured; some was relayed by R.S. when she spoke to law enforcement. I have personally reviewed the video from the event. Upon his arrival, MCQUESTION approached the door of R.S.'s residence and rang the doorbell. R.S. responded to the door, opened the front door but left the screen door locked as she spoke with MCQUESTION. MCQUESTION told R.S. that "I'm law enforcement, I'm FBI, Special Agent Harry Miller. Are you [R.S.]? I'm sorry about this I have a warrant for your arrest, you have to come with me." As the MCQUESTION identified himself as a Special Agent with the FBI, he proceeded to present what appears in the video to be official law enforcement credentials. R.S. asked MCQUESTION what the warrants were for. MCQUESTION stated that R.S. had two warrants for her arrest: one for drugs and one for prostitution. R.S. said she needed to confirm his claims via telephone with law enforcement. At that point, MCQUESTION left the scene. Flight records show that MCQUESTION flew back to Madison the following day.

12. After the encounter, R.S. used Google to search MCQUESTION's name from the certified letters he previously sent her. R.S. viewed MCQUESTION's photograph on his LinkedIn profile and it matched the person who came to her door and claimed to be a FBI agent. I also reviewed the security footage and could clearly view MCQUESTION's face when he was at R.S.'s door. I then reviewed MCQUESTION's LinkedIn account and recognized him as the same person who was at R.S.'s door on November 4, 2023. I also looked at MCQUESTION's photograph from his Wisconsin Driver's License and again confirmed that he is the person who was at R.S.'s door on November 4, 2023.

13. R.S. has stated that MCQUESTION's actions described above placed her in fear of serious bodily injury and caused her substantial emotional distress.

14. Based on my search of multiple databases, I know that MCQUESTION is not currently, nor has he ever been, employed by the Federal Bureau of Investigation, as a Special Agent or otherwise. My search of MCQUESTION's work history showed that he worked for Multiplan Services Corp. at the time of the offense.

15. The Subject Premises is the current residence of McQUESTION. FBI agents from Madison conducted surveillance at the Subject Premises and saw MCQUESTION at the Subject Premises on multiple occasions, as recently as March 31, 2023. While conducting surveillance, agents saw a vehicle registered to MCQUESTION parked in the reserved spot for the Subject Premises on multiple occasions, including March 31, 2023. Based on their surveillances, agents know that MCQUESTION works from the Subject Premises and does not go to a business or office location. Furthermore, Amazon records show that MCQUESTION uses the Subject Premises address for his Amazon account. Additionally, the Subject Premise was reported as MCQUESTION's current residence in October 2022 by Experian and Transunion and in December 2022 by Equifax.

16. In my training and experience, and based on conversations with senior FBI agents who have experience with these types of offenses, persons who impersonate federal officers keep indicia of such impersonation, like the fake law enforcement credentials McQUESTION showed to R.S., even after they have used the indicia. Persons who engage in stalking and interstate travel for such purposes keep evidence of those activities like travel records, records and results of location/background searches, and financial records related to those activities in paper copies and on electronic devices like computers, phones, and tablets. Persons engaged in these types of

activities would not normally keep them in a place of business and thus I believe there is probable cause to believe that such evidence would be found in the Subject Premises.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

17. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Subject Premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

18. *Probable Cause.* I submit that if a computer or storage medium is found on the Subject Premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, computer's internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache".

19. *Forensic Evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Subject Premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the

times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on

a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or mobile phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

20. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data at the Subject Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

22. I know that data files, including digitized images, correspondence, records, communications, and other matters sought by this Warrant can be stored in a variety of digital formats on a computer using various software applications. For example, digital still images are commonly created and stored as JPEG files and identified by .jpg or .jpeg in the filename suffix. Digital still images may also be created, converted, or stored, among other things, as an Adobe Acrobat file (using the suffix .pdf); embedded within a word processing document (using the suffix

.wpd, .doc or .docx); or converted to another graphics file format (.gif or .tif). In addition, data filenames typically include a suffix associated with the application that created or modified the file (e.g., XXXX.pdf indicates a file associated with Adobe Acrobat). A filename, however, can be manipulated to include a suffix that conceals its true format, or is not readily recognized by or associated with any software application. Accordingly, because digitized versions of items sought by this Warrant can be created and/or stored in any number of digital file formats, it is necessary to search every data file stored on a computer or other data storage device to locate and seize such items.

23. Mobile communication devices are commonly used for both personal and business use. These devices range from simple mobile telephones to complex devices encompassing numerous technologies in one hand-held device. They are electronically powered and typically combine the ability to store and transfer data along with serving as a communications facility. Mobile communication devices are essentially ultra-small computers, as proven by the following facts:

a. Mobile communication devices use microprocessors similar to computers. These processors are produced by the same companies that produce them for computers, like Intel, for example. The user interfaces with the device using a keyboard, much like a typical laptop or desktop computer and uses a directional pointer, much like a computer mouse.

b. The various technologies that can be incorporated into these devices include: telephones, still cameras, video cameras, Internet access (including e-mail, web surfing, file transferring), wireless data transfer between devices (such as Bluetooth technology, cellular transmission and infrared), data storage (including text files, image files, video files, spreadsheets, databases), data organizers (address, telephone, calendar), messaging, audio recorders, and music

players (such as MP3 players). The picture quality of images viewed on these devices can be quite excellent, as technology allows high resolution, color images, both still and video, to be viewed.

c. Mobile communication devices require the user to subscribe to services from a service provider. Such services can include telephone service (and all associated services such as voice mail, call waiting, caller ID, call forwarding, contact or address book), e-mail, Internet access, text messaging, data transfer (including the ability to transmit digital images and videos), and other fee-based services.

d. Mobile communication devices can communicate with other devices such as computers, telephones, personal digital assistants (PDAs), electronic peripherals such as printers, other mobile communication devices, and other such electronic or digital based devices. The methods typically used to connect with other devices include radio signals, Bluetooth wireless technology, and infrared (IR) signals.

e. Mobile communication devices generally use one of two popular operating systems, Android and Apple iOS. These operating systems allow the device to operate properly and to communicate with other devices. Both Android and Apple iOS have a component which is loaded onto a computer. This allows the user to enter or change data using the computer or the device, then transfer this data easily to/from the computer and the device. The procedure is called synchronization. The devices are typically sold with a cable which allows the user to synchronize the data on the device with their computer. These devices can also connect with a computer via infrared or network Internet Protocol (IP), allowing the user to synchronize with the host computer from anywhere a cellular connection is made.

f. Mobile communication devices also have what is called "volatile memory" similar to computers. Volatile memory allows data to be stored while the device is powered on,

then removes the data once the device is turned off. Not all data is stored in volatile memory, however, data can also be stored (and typically is stored) on memory cards. Mobile communication devices use memory cards just as a computer uses a hard drive. Once a memory card is inserted into the device, the user may store data on that card indefinitely, up to the storage capacity of that card. These cards can store up to 8 gigabytes of data. A card of this size could theoretically hold thousands of image files. The card may be removed and kept to use later, while another card may be inserted into the device. In this way, a user can have numerous cards storing volumes of data, any of which he can insert into a device when he wishes to access that data.

g. These devices are readily available to the public and are priced in a wide range allowing individuals from all economic levels to obtain the devices and the services associated with the devices.

h. Based on my training and experience involving mobile communication devices, I know these devices are commonly transported by the user on their person, in the user's vehicle, and are connected to the user's computer or computers via a USB connection cable. Users typically maintain software to communicate with the mobile communication devices on the residence and work computers and then transfer or synchronize the data on the device with the data on the computers. The purpose of this procedure is so the user has all data on the device and any and all computers at the user's disposal. This data can include personal or business contacts, calendar entries, notes or memos, and images. Users typically transport the device between their residence and business on a daily basis. As this device serves as a mobile telephone, users typically carry the device on their person and maintain it nearby when at work or home. It is the practice of many users to connect the device to the synchronization cable attached to their computer(s) while at home or work, for the most efficient transfer of data and updating of their files. I have has been

involved in cases where mobile communication devices have contained images downloaded from a personal computer.

24. Based on my training and experience, I know that mobile phones can be used to transmit both written messages ("texting") as well as images and/or videos. Mobile phones have the capacity to store voice mail messages, names, telephone numbers, addresses, sent and received text messages, and images on their internal memory. Many mobile phones have the capability to capture digital photographic images and videos, store them in internal memory, and transmit them to one or more different mobile phones. Some mobile phones contain small removable memory cards that can be used to store data and images.

CONCLUSION

25. Based on the aforementioned facts, there is probable cause to believe that one or more violations of 18 U.S.C. §§ 912 and 2261A (Impersonating a Federal Officer and Stalking) have been committed and that evidence, fruits, contraband, and instrumentalities of said offenses, as described in Attachment B, may be found at the Subject Premises. I respectfully request authority to seize such material.

26. Accordingly, I respectfully request this Court issue a search warrant for the Subject Premises, more particularly set forth in Attachment A, authorizing the search and seizure of the items listed in Attachment B.

27. It is respectfully requested that this Court issue an order sealing, until further order of this Court, all papers submitted in support of this application, including the application, affidavit, and search warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the Subject Premises). Sealing is necessary because the items and information to be seized are relevant to an ongoing

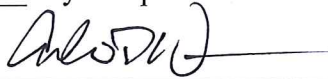
investigation, and premature disclosure of the contents of this Affidavit and related documents may jeopardize the effectiveness of the ongoing investigation.

Dated this 17th day of April 2023.

/s/

Sandra Jenkins
FBI, Special Agent

Sworn to me telephonically this 18th day of April 2023.

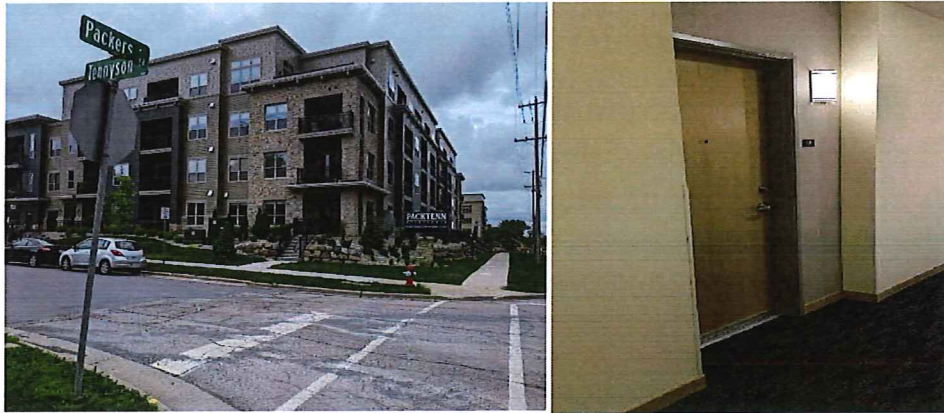


ANDREW WISEMAN
United States Magistrate Judge

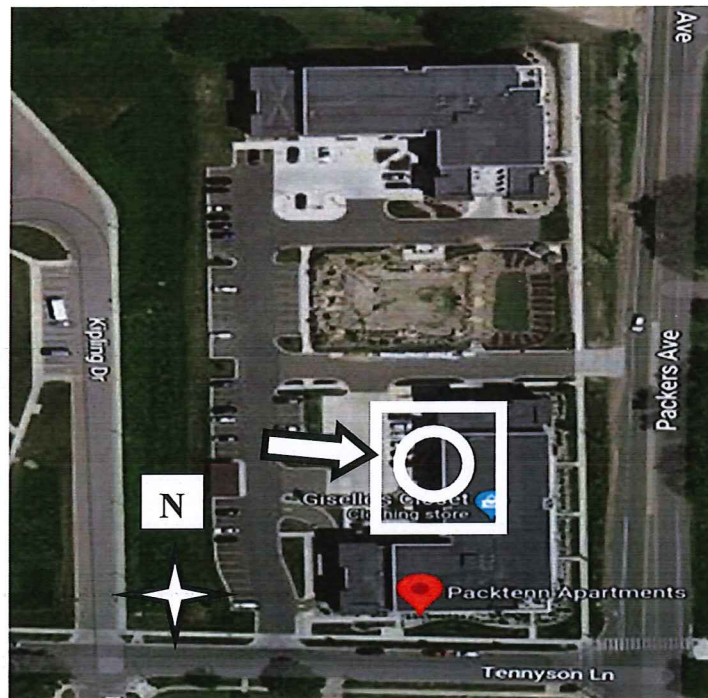
ATTACHMENT A

PROPERTY TO BE SEARCHED

The Subject Premises, **2024 Tennyson Lane #420, Madison, WI 53704**, is an apartment within the PackTenn apartment complex located at the northwest corner of the intersection of Tennyson Lane and Packers Avenue. The main entrance to the apartment complex is on the north side of Tennyson Lane. The Subject Premises is located within the building on the fourth floor. The following are recent photographs of the apartment complex entrance and the front door of the Subject Premises:



The following is an aerial image recently extracted from Google Maps of the general location of the PackTenn apartment complex in which the Subject Premises is situated. The PackTenn apartment complex is identified by a white rectangle and a white arrow. The white rectangle and white arrow are used merely to indicate the general location of the apartment complex within which the Subject Premises is situated and are not intended to define the actual or exact legal boundaries of the Subject Premises or the boundaries of the authorized search location.



ATTACHMENT B

ITEMS TO BE SEIZED AND SEARCHED

Items to be seized include all evidence relating to violations of 18 U.S.C. § 912 (Impersonating a Federal Officer) and 18 U.S.C § 2261A (Stalking). This evidence includes the following:

1. Any badges, identification documents, identity cards, insignia, seals, or records purporting to be issued by any department of the United States federal government or any state or local law enforcement entity, and any records or documentation (including electronic records or documentation) bearing the seal or insignia of any department or agency of the United States federal government.
2. Any clothing, equipment (e.g., tactical/utility vest, etc.), that bear indicia (e.g., insignia, lettering, wording, patterns, decals, seals, etc.) associating them with any department or agency of the United States federal government or any state or local law enforcement entity, including generic indicia (e.g., "FBI", "POLICE", "SWAT").
3. Any and all clothing worn by the Subject during the committal of Impersonating a Federal Officer.
4. Any pictures depicting law enforcement affiliations.
5. Evidence of the purchase of law enforcement related items.
6. All evidence relating to research regarding the location or activities of another person in relation to the subject offenses, including internet searches, mapping application searches, and communication with third parties.
7. All evidence of the Subject's travel to Austin, Texas, including but not limited to financial records, travel reservations, rental car receipts, and hotel receipts.

8. All evidence, including emails, text messages, and social media communications, about or to R.S.
9. All evidence regarding the Subject's location history.
10. Any emails regarding or referencing R.S., her location, or efforts to determine her location.
11. Any communications or records, whether physical or electronic, relating to working for/ with, or serving in, any agency or department of the United States federal government, or any state or local law enforcement agency.
12. Electronic devices, including cellular telephones, computers, and other devices containing electronically stored information and/or memory which could potentially contain items of evidence as described in this Attachment B.
13. As used above, the terms "records," "documents," and "items" include all forms of creation or storage, including paper format and electronic/digital format contained on computers* or electronic storage media.**

* For the purpose of this Attachment B and the associated search warrant, "computers" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices capable of performing logical, arithmetic, or storage functions, such as tablet devices, mobile phones, servers, laptop, notebook and desktop computers.

** For the purpose of this Attachment B and the associated search warrant, "electronic storage media" include: hard drives and portable hard drives of any kind, portable data storage devices such as thumb drives, SD cards, and DVD/CDs, network attached storage units, RAM, cyber wallets, cold storage digital currency wallets, or other media that can store digital and electronic data.